UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

REIS, INC. and REIS SERVICES, LLC,

Plaintiffs,

—against—

LENNAR CORP., RIALTO CAPITAL MANAGEMENT, LLC, and RIALTO CAPITAL ADVISORS OF NEW YORK, LLC,

Defendants.

15 Civ. 7905 (GBD)

REIS'S MEMORANDUM OF LAW
IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Table of Contents

TABLE OF AUTHORITIES

Statutes

Other Authorities

I. INTRODUCTION

As Defendants point out, this is one of nine lawsuits that Reis has filed in this District against businesses that have downloaded its proprietary commercial real estate reports without authorization. The other suits have generally settled or proceeded to discovery – and for good reason. It is beyond reasonable dispute that using a stolen or misappropriated password to obtain proprietary data without paying for it is contrary to the law. As Reis alleges in the complaint, that is what Defendants did here. Not only must these allegations be accepted as true for purposes of this motion, they are demonstrably true. Reis's computer records show that the Defendants downloaded over $1.6 million worth of commercial real estate data using a password that had been issued to the former employer of one of Defendants' employees. At trial, Defendants will be in no position to contest this fact.

Given this indisputable evidence, it is not surprising that Defendants have taken a shot at moving to dismiss the complaint. The motion misfires because Defendants' fraudulent misappropriation of Reis's data plainly gives rise to liability under federal and state law. As explained below, Defendants' conduct meets all the elements of the causes of action alleged in the complaint: violation of the Computer Fraud and Abuse Act ("CFAA"), fraud, conversion, misappropriation, breach of contract, unjust enrichment, quantum meruit, and contributory and vicarious copyright infringement.

Before detailing the defects in Defendants' arguments, it is worth pausing to consider the extraordinary legal proposition underlying their motion. Defendants accept for purposes of this motion (and ultimately will not be able to dispute) that they downloaded thousands of proprietary commercial real estate reports from Reis's database, using login credentials that they were unauthorized to use, without paying for it. In moving to dismiss the complaint in its entirety, Defendants are taking the position that this behavior is *entirely permissible*—that Reis has no legal recourse against the flagrant data piracy alleged in the complaint. This proposition is untenable. If Reis can prove its allegations that Defendants stole its data (and it can) it will be entitled to a remedy. Defendants' motion should be denied.

II. FACTUAL ALLEGATIONS

Reis's complaint describes two separate sets of data piracy by Defendants. The first involves approximately $1.6 million worth of data taken by Defendants Lennar Corporation ("Lennar") and Rialto Capital Management, LLC ("Rialto"). The second involves about $277,000 worth of data misappropriated from the Reis account of Defendant Rialto Capital Advisors of New York, LLC ("Rialto New York").

A. Unauthorized Use of Harvey Lederman's Reis Credentials by Lennar and Rialto

The first and larger set of unauthorized usage involves the downloading of more than $1.6 million worth of Reis reports using Reis login credentials issued through the former employer of a Rialto employee. Compl. ¶¶ 4, 31–35. The Rialto employee, Harvey Lederman,[1] worked for a company that subscribed to Reis before joining Rialto in October 2009. *Id.* ¶¶ 4, 31. Between December 2009 and October 2010, Defendants used the Reis username and password issued to Mr. Lederman's previous employer to access the Reis database and download 4,548 Reis reports with a retail value of $1,629,948. *Id.* ¶ 32. During this time, none of the Defendants had a license to use the Reis database. *Id.* ¶ 35.

Only Defendants know for certain why they used another company's Reis login credentials to download thousands of proprietary reports from Reis. According to available evidence, however, the information appears to have been used by Lennar, traditionally a

[1] Defendants assert that Mr. Lederman is employed by Rialto New York, and "does not work for Rialto or Lennar." Def. Br. at 4 n.3. Notably, Defendants do not assert that Mr. Lederman worked for Rialto New York at the time of the allegations in the complaint. Mr. Lederman's Linked-In page lists his employer as Rialto Capital Management. *See* https://www.linkedin.com/in/harveylederman (Dec. 22, 2015).

homebuilder, to launch a commercial real estate investing business under the Rialto name. In January 2011, Lennar announced that the fourth quarter of 2010 had witnessed the "first closing of our Rialto real estate investment fund with initial equity commitments of approximately $300 million (including $75 million committed by us)." *Id.* ¶ 34. In November 2010, Defendant Rialto New York entered into a Reis subscription. *Id.* ¶ 35. Both these events occurred immediately after the Lederman unauthorized usage ceased in October 2010.

Until this year, Reis did not know that the Lederman usage between December 2009 and October 2010 had been on behalf of Defendants. *Id.* ¶ 31. Because Mr. Lederman's credentials were issued by his former employer, the usage appeared to Reis to be on behalf of that employer. Recently, however, a spate of piracy led Reis to scrutinize its records more carefully to identify unauthorized usage. *Id.* ¶ 33. In June 2015, Reis discovered that Mr. Lederman had been employed by Rialto beginning in October 2009, and that the usage from his former employer's account was associated with Defendants. *Id.* ¶¶ 31, 33.[2]

B. Rialto New York's Unauthorized Sharing of Reis Credentials

The second group of allegations in the complaint involves the use of Defendant Rialto New York's Reis login credentials from unknown Internet Protocol ("IP") addresses to download approximately $277,000 worth of Reis reports in 2015. *Id.* ¶¶ 6–7, 36–37. In recent years, Reis's Compliance Group has been investigating unusual patterns of use and other signs of possible theft of data from the Reis database. *Id.* ¶ 33. These investigations uncovered that, between May 2013 and August 2015, unidentified persons associated with two IP addresses—67.136.101.2 and 173.11.106.97—used Rialto New York credentials to download at least 747

[2] Defendants contend that Reis learned that Harvey Lederman worked for Rialto in November 2010. Def. Br. at 5, 11–12. They do not contend that Reis was informed that Mr. Lederman worked for Rialto before November 2010. As explained below, the suggestion that this information should have led Reis to discover that earlier usage on a different account issued in the name "Harvey Lederman" was unauthorized is baseless.

reports from the Reis database with a retail value of $277,412. *Id.* ¶ 36. These two IP addresses are not associated with Rialto New York and their associated usage patterns are not consistent with simple explanations such as an employee logging in remotely. *Id.* Reis's subscriber agreement with Rialto New York, which incorporates Reis's Terms of Service, strictly prohibits the sharing of Reis login credentials. *Id.* ¶ 37. The unauthorized users of Rialto New York's credentials are referred to as the "Doe Unauthorized Users."[3]

III. ARGUMENT

A. Legal Standard

A Rule 12(b)(6) motion to dismiss must be denied if the complaint states "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims." *Walker v. Schult,* 717 F. 3d 119, 124 (2d Cir. 2013) (citations omitted). "In ruling on a motion [to dismiss] the duty of a court is merely to assess the legal feasibility of the complaint, not to assay the weight of the evidence which might be offered in support thereof." *DiFolco v. MSNBC Cable L.L.*C., 622 F.3d 104, 113 (2d Cir. 2010) (citation and internal quotation marks omitted)).

B. Reis Has Properly Pleaded Claims Against Lennar and Rialto Based on the Lederman Usage

1. The Complaint States a Claim Under the Computer Fraud and Abuse Act

Despite asserting that the CFAA "has no application here" (Def. Br. at 8), Defendants do not actually dispute that Reis has alleged a violation of the statute. "The CFAA criminalizes,

[3] After the complaint was filed, the Court granted Reis permission to issue subpoenas to the internet service providers whose IP addresses were used by the Doe Unauthorized Users. The information shows that the Doe Unauthorized Users are commercial real estate firms, one of which is affiliated with Defendants (but is not a Reis subscriber), the other of which is independent. Caplan Decl. Exs. B and D.

inter alia, 'intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer.'" *Sewell v. Bernardin*, 795 F. 3d 337, 339–40 (2d Cir. 2015) (quoting 18 U.S.C. § 1030(a)(2)(C)). Defendants do not contest that by accessing Reis's database using the login credentials of Mr. Lederman's former employer, they obtained information from a protected computer without authorization in violation of the CFAA. Indeed, it is beyond dispute that a former employee violates the CFAA by accessing a proprietary database using his former employer's credentials.[4]

Unable to defend the legality of their conduct, Defendants contend that Reis has failed to plead that it meets the jurisdictional requirements for a civil action under the CFAA or the statute of limitations for CFAA claims. To the contrary, Reis has alleged these requirements in substantial detail.

a. Reis Has Properly Alleged a "Loss" of At Least $5000

The CFAA allows for civil actions to enforce its requirements, but only if the offense involves at least one of a specified set of factors. *See* 18 U.S.C. §1030(g). One of these factors is whether the conduct in question caused a "loss" to the plaintiff "aggregating at least $5,000 in value" over one year. 18 U.S.C. § 1030(c)(4)(A)(i)(I). The CFAA defines "loss" as "[1] any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior

[4] *See, e.g., University Sports Publ'ns. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 385–86 (S.D.N.Y. 2010) ("All parties agree that if Pitta accessed the database after he left USP's employ in 2006, he did so 'without authorization.'"); *Lvrc Holdings LLC v. Brekka*, 581 F. 3d 1127, 1136 (9th Cir. 2009) ("There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA."). *See also United States v. Valle*, 2015 U.S. App. LEXIS 21028 (2d Cir. Dec. 3, 2015) (noting that "effectively all computers with Internet access" are "protected computers" under the CFAA) (quoting *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012)).

to the offense, and [2] any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Here, Reis alleges that it has incurred costs far in excess of $5,000 responding to Defendants' offense, including by conducting an investigation into the extent of the unauthorized use, developing and enhancing software to identify hidden piracy by Defendants and others, and using the software to monitor Defendants' usage. Compl. ¶¶ 47–54. Reis has properly pleaded a civil action under the CFAA.

Defendants' primary argument is that lost revenue only constitutes a "loss" under the CFAA when it results from an interruption of service. Def. Br. at 8–10. This argument is beside the point. For purposes of this motion, Reis does not rely on its lost revenue to satisfy the "loss" requirement of the CFAA. Rather, Reis relies on its allegations regarding the costs of investigating and responding to Defendants' unauthorized access. *See* Compl. ¶¶ 47–54. Appropriately, Defendants do not contend that these costs must be tied to an interruption of service. *See*, *e.g.*, *University Sports*, 725 F.Supp.2d at 387 (holding that "the costs of investigating security breaches constitute recoverable 'losses,' even if it turns out that no actual data damage or interruption of service resulted from the breach").

Defendants argue that Reis's investigative costs do not count as "losses" under the CFAA because they relate to "business losses" rather than "damage" to "data, programs, systems, or information." Def. Br. at 10. This argument is contrary to the statutory text, which defines a loss as "any reasonable cost to any victim, including the cost of responding to an offense," and is not limited to computer damage. 18 U.S.C. § 1030(e)(11). Thus, the "weight of case law holds that a Plaintiff can satisfy the CFAA § 1030(g) 'damage or loss' requirement by pleading a loss stemming from a damage assessment and/or remedial measures, even without pleading actual damage" to its computer systems. *Ipreo Holdings LLC v. Thomson Reuters Corp.*, 2011 U.S. Dist. LEXIS 25356, at *22 (S.D.N.Y. Mar. 7, 2011).[5]

The Second Circuit summary order on which Defendants rely, *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559 (2d Cir. 2006), is not to the contrary. *Nexans* held that travel expenses incurred by company executives to attend a business meeting were not "losses" under the CFAA because the meeting was unrelated to "any type of computer investigation." *See id.* at 563. Here, in contrast, Reis is relying on the costs of computer investigations necessitated by Defendants' unauthorized access to its database. Compl. ¶¶ 47–54. These costs are losses under the plain language of 18 U.S.C. § 1030(e)(11).[6]

Finally, Defendants contend that even if Reis's allegations constitute losses under the CFAA, they are "belied" by the fact that Reis has relied on the same software development expenses in other lawsuits. Def. Br. at 10–11. This argument suffers from failures of reading and arithmetic. Contrary to Defendants' allegations of improper pleading (Def. Br. at 1), the complaint makes clear that the software in question was developed to "investigate intrusions into its computer system by the Defendants *and others*." Compl. ¶ 50 (emphasis added); *accord id.* ¶¶ 51–53. The complaint also makes clear that the development of investigative software is only one component of Reis's costs, and that more than $5,000 worth of investigative efforts were

[5] *See also University Sports*, 725 F.Supp.2d at 388 (holding that an audit "investigating defendants' alleged crimes [which] sought to identify evidence of the breach, assess any damage it may have caused, and determine whether any remedial measures were needed to resecure the network" constituted "loss" under the statute); *Kaufman v. Nest Seekers, LLC*, 2006 U.S. Dist. LEXIS 71104, at *25 (S.D.N.Y. Sept. 26, 2006) ("The claimed loss sustained by PCL and BrokersNYC in investigating the potential damage to their computer system and Website is not lessened merely because fortuitously no physical damage was allegedly caused to the computer system or software.").

[6] *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805 (N.D. Ill. 2009), also relied on by Defendants, is a summary judgment opinion. The court expressly noted that "[t]his is not a motion to dismiss" and held that the testimony of plaintiff's witness was insufficient to establish loss under the CFAA. *Id.* at 812. If this Court were to accept the reasoning of *Del Monte*, that case would call for denying Defendants' motion to dismiss and proceeding to discovery.

devoted specifically to Defendants in one calendar year. *Id.* ¶ 54. Even if the $76,364 Reis spent on investigative software were divided evenly among the nine lawsuits it has filed, moreover, simple arithmetic shows that more than $5,000 of these costs would be attributable to Defendants. *Id.* ¶ 49. In any event, Defendants are challenging Reis's evidence, not arguing that its allegations fail to state a claim. There is no basis to dismiss the CFAA claims.

b. The CFAA Claim Is Not Time-Barred

Defendants' statute of limitations argument also disputes facts rather than challenges the sufficiency of Reis's pleading. Def. Br. at 11–12. Defendants concede that the statute of limitations for CFAA claims is two years from "the date of the act complained of *or the date of the discovery of the damage*." 18 U.S.C. § 1030(g) (emphasis added); *Sewell*, 795 F. 3d at 338. Here, Reis alleges that it discovered Defendants' unauthorized usage in 2015. Compl. ¶¶ 6, 33. Reis's CFAA claim is therefore timely.

Defendants contend that Reis's allegation is "false" because in November 2010—after the unauthorized usage in question—Defendants included the name of Harvey Lederman in a list of authorized users under the Rialto New York-Reis contract. Def. Br. at 12. This is an argument for summary judgment or trial. It is also exceedingly weak. Rialto New York's listing of its authorized employees was entirely innocuous and provided no reason for Reis to initiate an investigation into possible unauthorized usage. Furthermore, Reis had no way to know that the "Harvey Lederman" identified by Rialto New York was the same Harvey Lederman whose name appeared in the fine print of one of the hundreds of other Reis contracts with different companies. Even if Reis had made this unlikely connection, the only way it would have learned that Mr. Lederman's prior usage was for Defendants and not for his former employer would have been to trace the IP address from which he had previously accessed the Reis database. As Reis alleges in the complaint, it was not actively investigating unauthorized use in this way because it was not yet aware of the extent of its data piracy problem. Compl. ¶¶ 6, 33. Simply put, Defendants' CFAA statute of limitations argument fails.

2. Reis Has Properly Pleaded Fraud Based on Defendants' Misrepresentations About Their Identity and Corporate Affiliation

Defendants' attempt to dismiss the fraud claim also fails. The elements of a fraud claim under New York law are: "(1) a material misrepresentation or omission of a fact, (2) knowledge of that fact's falsity, (3) an intent to induce reliance, (4) justifiable reliance by the plaintiff, and (5) damages." *Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC*, 797 F.3d 160, 170 (2d Cir. 2015). To satisfy the pleading requirements of Rule 9(b), "a party must state with particularity the circumstances constituting fraud or mistake," but "[m]alice, intent, knowledge, and other conditions of a person's mind may be alleged generally." Fed. R. Civ. P. 9(b); *see also Loreley*, 797 F.3d at 170–71.

Reis's complaint easily meets these requirements. The fraud is alleged with particularity: Defendants logged into the Reis database using the login credentials issued to Harvey Lederman by his former employer. Every time agents of Defendants did this, they were representing (i) that they were Mr. Lederman, and (ii) they were affiliated with his previous employer. *Id.* ¶ 93. At least the second point was knowingly false – "not least because entering [Mr. Lederman's] credentials required entering [his] work e-mail address from his previous employer" into the username field. *Id.* Defendants' sole purpose in misrepresenting their identity and/or company affiliation to Reis was to induce Reis to provide access to its database, which it did, suffering damages in the form of lost revenues.

a. Rule 9(b) Does Not Require Reis to Identify the Particular Individual(s) Who Lied to Reis

Defendants argue that Reis has failed to "identify the individual(s)" who used the Lederman credentials on behalf of Defendants. Def. Br. at 15. This argument qualifies as chutzpah. The reason Reis does not know exactly who misappropriated Mr. Lederman's login credentials is that the credentials were misappropriated. As far as Reis was informed, its database was being accessed by Mr. Lederman on behalf of his former employer. This information turned out to be false. What Reis now knows is that Mr. Lederman either (a) misrepresented his company affiliation, (b) gave his Reis credentials to colleagues who mispresented their identities *and* company affiliation, or (c) both. All of these possibilities constitute fraud. Only the Defendants know which of them is true. *See Sullivan v. Kodsi*, 373 F. Supp. 2d 302, 306 (S.D.N.Y. 2005) ("Where facts are peculiarly within the opposing party's knowledge … a complaint may base allegations on information and belief.").

Rule 9(b) does not require the plaintiff to identify the responsible individual in these circumstances. Where, as here, there is the possibility of plural authorship of the fraudulent statements, "there is no fixed requirement … to identify a single entity within the group on pain of dismissal." *Loreley*, 797 F.3d at 173; *see also Arenson v. Whitehall Convalescent & Nursing Home*, 880 F. Supp. 1202, 1208 (N.D. Ill. 1995) ("[W]here a complaint involves allegations of corporate fraud, the particularity requirement may be relaxed where it is difficult to attribute particular fraudulent conduct to each defendant as an individual.") (internal quotation marks omitted).[7] That is the only reasonable rule. Allowing Defendants to avoid liability by concealing their identities would make no sense at all. *See Bigelow v. RKO Radio Pictures, Inc.*,

[7] This same line of authority disposes of Defendants' specious argument (Def. Br. at 25) that Reis fails to state a claim against Lennar. *See also Luce v. Edelstein*, 802 F.2d 49, 55 (2d Cir. 1986).

327 U.S. 251, 264–65 (1946) (rejecting a "rule [that] would enable the wrongdoer to profit by his wrongdoing at the expense of his victim").

b. Reis Adequately Pleads Scienter

Defendants' argument that they did not "actually" know their usage was unauthorized (Def. Br. at 15) fails as a matter of law and common sense. Under Rule 9(b), scienter may be "alleged generally." Fed. R. Civ. P. 9(b). The complaint must only plead facts "which give rise to a strong inference that the defendant had an intent to defraud, knowledge of the falsity, or a reckless disregard for the truth." *Cohen v. S.A.C. Trading Corp.*, 711 F.3d 353, 359 (2d Cir. 2013) (quoting *Caputo v. Pfizer, Inc.*, 267 F.3d 181, 191 (2d Cir. 2001)) (internal quotation marks omitted). A plaintiff meets the "strong inference" standard "either (a) by alleging facts to show that defendants had both motive and opportunity to commit fraud, or (b) by alleging facts that constitute strong circumstantial evidence of conscious misbehavior or recklessness." *Intelligen Power Sys., LLC v. dVentus Techs., LLC*, 2015 U.S. Dist. LEXIS 71078, at *35 (S.D.N.Y. June 2, 2015); *see also Loreley*, 797 F.3d at 177.

The allegations in the complaint satisfy both of the alternative tests for pleading scienter. Lennar and Rialto had both opportunity (Mr. Lederman's credentials) and a motive (avoiding a costly subscription to the Reis database) to lie about their authorization to use the Reis database. Indeed, they avoided $1.6 million in costs by doing so. Compl. ¶¶ 1, 32, 94. The allegations in the complaint also establish "strong circumstantial evidence of conscious misbehavior or recklessness." Reis alleges that Defendants' representation that they were authorized to use Mr. Lederman's login credentials "was false each time it was made, and the user making it knew it was false each time it was made, *not least because entering [Mr. Lederman's] credentials required entering [Mr. Lederman's] work e-mail address from his previous employer*." Compl. ¶ 93 (emphasis added). Whether or not they are aware of Reis's Terms of Service, anyone who logs into a proprietary database using login credentials issued to a different company knows that they are misrepresenting their corporate affiliation. That somebody at Lennar or Rialto did this more than 4,500 times is not an honest mistake.

c. Reis's Reliance Was Reasonable

Finally, Defendants argue that Reis's reliance on the representations made at the login screen was not reasonable, because Reis should have independently discovered Defendants' fraud. Def. Br. at 15–17. Whether the plaintiff's reliance is reasonable is a "fact-intensive inquiry" that usually "cannot be decided on [a] motion to dismiss." *Oneida Sav. Bank v. Uni-Ter Underwriting Mgmt. Corp.*, 2014 U.S. Dist. LEXIS 130677, at*39 (N.D.N.Y. Sept. 18, 2014) (quoting *Sawabeh Info. Servs. Co. v. Brody*, 832 F. Supp. 2d 280, 304 (S.D.N.Y. 2011)). Here, Defendants' contention that Reis's reliance was unreasonable borders on the absurd.

Like many electronic resources, Reis's database can be accessed by entering a valid password. With thousands of users accessing the database millions of times per year, Reis cannot possibly make real-time, individualized assessments as to whether a given user bearing a valid password is in fact authorized to use it. Reis takes steps to ensure the integrity of its password system by protecting its database with a firewall, requiring that usernames and passwords be administered through the subscriber, and requiring that all subscribers abide by Reis's Terms of Service, which strictly prohibit the sharing of Reis IDs. *Id.* ¶¶ 25–28. Relying on Defendants' possession of a working password to provide them access to the Reis database was plainly reasonable.

Defendants suggest that because Reis was ultimately able to discover their fraud, it never should have fallen for it in the first place. Def. Br. at 16–17. In addition to being self-refuting, this argument is contrary to the allegations in the complaint. As Reis alleges, it was not until a recent rise in piracy led Reis to increase its compliance investigations that it was able to identify the suspicious usage patterns that signaled Defendants' fraud. Compl. ¶ 33. Furthermore, Reis's ability to use investigative tools to uncover unauthorized usage that has already occurred does not mean that Reis has the ability to prevent such piracy at the time it happens. Reis's fraud claim easily survives Defendants' motion to dismiss.

3. Reis's Terms of Service Are Enforceable Against Lennar and Rialto

Reis pleads contract claims against Lennar and Rialto based on the Terms of Service that are displayed prominently on its website. Compl. ¶¶ 30, 97. The Terms of Service are also incorporated into the contract under which Mr. Lederman's credentials were issued and Mr. Lederman was required to agree to them as a user of the Reis database. *Id.* ¶¶ 27, 28.

Defendants cannot dispute that they breached the Terms of Service by using Reis login credentials issued to Mr. Lederman by his former employer. Instead, they argue that Reis's claims must be dismissed at the pleading stage because Defendants never "exhibit[ed] 'unambiguous assent'" to the Terms that prohibit their conduct. (Def. Br. at 13 (quoting *Berkson v. Gogo LLC*, No. 14-CV-1199, 2015 WL 1600755, at *26 (E.D.N.Y. Apr. 9, 2015), *corrected opinion reported at* 97 F. Supp. 3d 359)). Defendants' reliance on *Berkson* is misplaced. As the opinion makes clear, the *Berkson* standard applies where the Terms of Service are being enforced against a consumer. Courts have found it much easier to enforce browsewrap[8] agreements against corporations such as Defendants. *See Berkson*, 97 F. Supp. 3d at 396 ("courts generally have enforced browsewrap terms only against knowledgeable accessors, such as corporations"); *see also Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 836 (S.D.N.Y. 2012) ("the cases in which courts have enforced browsewrap agreements have involved users who are

[8] The word "browserap" refers to cases where "assent is given merely by using the site." *Berkson*, 97 F. Supp. 3d at 394.

businesses rather than … consumers") (citing Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 472 (2006)).

Assent to a browsewrap agreement can be inferred where sufficient facts have been pleaded to establish actual, inquiry, or constructive notice of the contract sought to be enforced. *See Berkson*, 97 F. Supp. 3d at 393 ("the contract-formation question will often turn on whether a reasonably prudent offeree would be on [inquiry] notice of the term[s] at issue") (quoting *Schnabel v. Trilegiant Corp.*, 697 F. 3d 110, 120, 126–27 (2d Cir. 2012)) (alterations in original); *id*. at 394 ("Inquiry notice is actual notice of circumstances sufficient to put a prudent man upon inquiry.") (quoting *Specht v. Netscape Communs. Corp.*, 306 F.3d 17, 30 n.14 (2d Cir. 2002)). Even in consumer cases, this is a fact-intensive inquiry. *See Berkson*, 97 F. Supp. 3d at 395 ("Because of the passive nature of acceptance in browsewrap agreements, courts closely examine the factual circumstances surrounding a consumer's use.").

Here, Reis sufficiently alleges both actual and constructive notice on the part of the corporate Defendants, who clearly were on notice that a duly assigned password was required to access the Reis database. Compl. ¶¶ 30, 97. Furthermore, Mr. Lederman's knowledge of Reis's Terms of Service, which derive not only from the website but also an agreement he needed to enter into to obtain credentials (*id.* ¶¶ 27, 28) can be imputed to Defendants. *See* Restatement (Third) of Agency § 5.03 ("[N]otice of a fact that an agent knows or has reason to know is imputed to the principal if knowledge of the fact is material to the agent's duties to the principal."). Indeed, courts have enforced browsewrap agreements in highly similar circumstances. *CoStar Realty Info., Inc. v. Feld*, 612 F. Supp. 2d 660, 668–69 (D. Md. 2009) (enforcing a forum selection clause in the terms of service of a Reis competitor under similar allegations); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 401 (2d Cir. 2004) (analogizing to an apple buyer who might not see the price before eating his first apple, but "c[ould] not continue on a daily basis to take apples for free, knowing full well that [seller] is offering them only in exchange for 50 cents compensation").[9] Defendants' motion to dismiss the breach of contract claim against Lennar and Rialto fails.

4. Reis's Alternative Claims for Quantum Meruit and Unjust Enrichment Are Valid and Timely

In the alternative to its breach of contract claim, Reis pleads claims sounding in quantum meruit and unjust enrichment, because Lennar has used its unauthorized access to receive the benefit of Reis's services without paying for those services. Compl. ¶¶ 143–71. It is well established that a plaintiff may plead contract and quasi-contract theories such as unjust enrichment and quantum meruit in the alternative to a breach of contract claim. *See Altaire Pharms., Inc. v. Rose Stone Enters.*, 2013 U.S. Dist. LEXIS 170411, at *19–20 (E.D.N.Y. Dec. 3, 2013) (collecting cases). Where the existence of a valid and binding contract between the parties is a subject of dispute, dismissal of such alternative claims is inappropriate. *See Knudsen v. Quebecor Printing (U.S.A.), Inc.*, 792 F. Supp. 234, 237 (S.D.N.Y. 1992) ("[W]hen the

[9] In contrast, the cases cited by Defendants did not involve situations where the terms of service in question were obvious from the circumstances and where the defendant had been required to agree to them separately from the browsewrap process. *See Berkson*, 97 F. Supp. 3d at 403–04 (rejecting defendants' motion to compel arbitration in consumer suits concerning in-flight Wi-Fi where defendant "did not make an effort to draw Berkson's attention to its 'terms of use,'" but allowing defendants' motions to be renewed after discovery is completed); *Hines v. Overstock.com, Inc.*, 380 F. App'x 22, 25 (2d Cir. 2010) (declining to compel arbitration against a consumer "because Overstock did not allege any facts tending to show that a user would have had actual or constructive knowledge of the Terms and Conditions"); *Be In, Inc. v. Google Inc*, 2013 U.S. Dist. LEXIS 147047, at *35–36 (N.D. Cal. Oct. 9, 2013) (disallowing a breach of contract claim because "Be In has not sufficiently alleged how its link would provide notice" but granting leave to replead); *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 936–37 (E.D. Va. 2010) (refusing to enforce Terms of Use that "only appear[ed] on Cvent's website via a link buried at the bottom of the first page"). *Fteja*, on which Defendants also rely, held that the contractual provision in question was valid. 841 F. Supp. 2d at 841.

existence of the contract is in dispute, a plaintiff may plead breach of contract and quantum meruit in the alternative.”).

Seizing on the fact that Mr. Lederman’s former employer had a valid contract with Reis that is not in dispute, Defendants argue that “there can be no quasi-contract claim against a third-party non-signatory to a contract that covers the subject matter of the claim.” Def. Br. at 20 (citing *Melcher v. Apollo Med. Fund Mgmt, L.L.C.*, 105 A.D.3d 15, 27–28 (1st Dep’t 2013); *SCM Grp., Inc. v. McKinsey & Co.*, 2011 U.S. Dist. LEXIS 31972, at *23 n.4 (S.D.N.Y. Mar. 28, 2011)). These cases are inapposite because Reis’s quasi-contract claims against Defendants do not cover the same subject matter as Reis’s contract with Mr. Lederman’s former employer. The agreement with Mr. Lederman’s former employer concerns use of the Reis database by users under that agreement. It does not cover use of the Reis database by Defendants. Defendants’ actions are governed by their own agreement to the Reis Terms of Service. By disputing the validity of that contract, Defendants subject themselves to Reis’s alternative quasi-contract theories. *See Hughes v. BCI Int’l Holdings, Inc.*, 452 F. Supp. 2d 290, 304 (S.D.N.Y. 2006) (“The Bridge Loan Agreements and promissory notes governed plaintiffs’ investment in [one of the defendants]. However, those agreements do not set forth plaintiffs’ rights and obligations with respect to [another group of defendants]”); *SungChang Interfashion Co. v. Stone Mountain Accessories, Inc.*, 2013 U.S. Dist. LEXIS 137868, at *54–58 (S.D.N.Y. Sept. 25, 2013) (“[A]lthough SungChang alleges breach of contract against SMA, this does not disturb its ability to also seek unjust enrichment against third parties by virtue of the alleged transfer.”).

Defendants’ contention that the unjust enrichment claim is governed by a three-year statute of limitations is mistaken. Def. Br. at 20–21. Unjust enrichment claims have a six-year statute of limitations. *See Cohen v. S.A.C. Trading Corp.*, 711 F.3d at 364 (noting that “[u]nder

New York law" there is a "six-year limitations period for unjust enrichment"); N.Y. C.P.L.R. § 213(1) (six-year statute of limitations for actions "for which no limitation is specifically prescribed by law"). The case cited by Defendants, *Grynberg v. Eni Sp.A.*, 2007 U.S. Dist. LEXIS 65787, at *9 n.11 (S.D.N.Y. Sept. 5, 2007), sets forth the minority view. *See Ross v. Thomas*, 2010 U.S. Dist. LEXIS 107748, at *20 (S.D.N.Y. Oct. 7, 2010) (collecting cases and noting that "[w]hile New York courts have occasionally applied a three-year statute of limitations to unjust enrichment claims, they more commonly apply a six-year statute of limitations"). The unjust enrichment claim is timely.

5. The Conversion Claim Is Legally Viable and Timely

Defendants argue that Reis may not state a claim for conversion or theft of its reports, because they are in electronic form and Reis has not been denied access to copies of the reports. Def. Br. at 17–18. Defendants are incorrect.

Conversion is the "'unauthorized assumption and exercise of the right of ownership over goods belonging to another to the exclusion of the owner's rights.'" *State of New York v. Seventh Regiment Fund.*, 98 N.Y.2d 249, 259 (2002) (quoting *Vigilant Ins. Co. of Am. v. Housing Auth. of City of El Paso, Tex.*, 87 N.Y.2d 36, 44 (1995)). Because the "tort of conversion must keep pace with the contemporary realities of widespread computer use," the New York Court of Appeals has expanded the tort to include certain intangible property, including electronic data. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 292 (2007).

New York State and federal courts have repeatedly invoked *Thyroff* to uphold claims of conversion of intangible property, including electronic records and documents. *See Volodarsky v. Moonlight Ambulette Serv., Inc.*, 122 A.D.3d 619, 620 (2d Dep't 2014) ("[E]lectronic documents stored on a computer may be the subject of a conversion claim just as printed versions of the documents may"); *New York Racing Ass'n v. Nassau Reg'l Off-Track Betting

Corp., 29 Misc. 3d 539, 545–46 (Sup. Ct. 2010) ("[P]laintiff may maintain an action for conversion where its electronically stored data is misappropriated, regardless of whether plaintiff has been excluded from access to its intangible property."); *Harris v. Coleman*, 863 F. Supp. 2d 336, 345 (S.D.N.Y. 2012) ("[B]ecause of the more recent adoption of the merger doctrine, intangible property may be subject to conversion when represented by a tangible manifestation, such as an electronic or paper record.").[10]

Defendants' argument that Reis's conversion claim is untimely also fails. Although Defendants are correct that conversion is ordinarily governed by a three-year statute of limitations, the limitations period is six years where, as here, the claim is based on allegations of fraud. *See Ingrami v. Rovner*, 45 A.D.3d 806, 808 (2d Dep't 2007) ("Contrary to the appellant's claim, the fraud and conversion causes of action are governed by the six-year statute of limitations contained in CPLR 213 (8) . . . ."); *Petrou v. Karl Ehmer Intl. Foods, Inc.*, 167 A.D.2d 338, 339 (2d Dep't 1990) (similar); N.Y. CPLR 213(8) (providing a six-year statute of limitations for causes of action "based upon fraud"). Because as discussed above Reis properly alleges fraud, the conversion claim is also timely.

6. Reis's Misappropriation Claims Are Properly Pleaded and Timely

Defendants move to dismiss Reis's misappropriation claims by mischaracterizing them as claims for trade secret protection. Def. Br. at 18–19. That is not the claim. Rather, Reis has alleged a common law misappropriation claim, which is a species of unfair competition. "It is

[10] In each of the cases cited by Defendants, the records stolen had no commercial retail value. *GEO Grp., Inc. v. Cmty. First Servs., Inc.*, 2012 U.S. Dist. LEXIS 45654 (E.D.N.Y. Mar. 30, 2012) (trade secrets); *Trustforte Corp. v. Eisen*, 10 Misc. 3d 1064(A) (Sup. Ct. 2005) (customer lists); *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 813 F. Supp. 2d 489, 536 (S.D.N.Y. 2011) (same). By contrast, here Reis lost control of a commodity having an established retail value. Although Reis may in some (but not all instances) be able to retain a copy of the report, Reis has been deprived of the retail value of the reports taken by Defendants.

well settled that 'the primary concern in unfair competition is the protection of a business from another's misappropriation of the business' 'organization [or its] expenditure of labor, skill, and money.'" *Macy's Inc. v. Martha Stewart Living Omnimedia, Inc.*, 127 A.D.3d 48, 56 (1st Dep't 2015) (quoting *Ruder & Finn. v. Seaboard Sur. Co.*, 52 N.Y.2d 663, 671 (1981)). Thus, "[a]llegations of a 'bad faith misappropriation of a commercial advantage belonging to another by exploitation of proprietary information' can give rise to a cause of action for unfair competition." *Macy's Inc.*, 127 A.D.3d at 56 (quoting *Out of Box Promotions, LLC v. Koschitzki*, 55 A.D.3d 575, 578 (2d Dep't 2008)). The parties need not be competitors in order to sustain a claim. Instead, the plaintiff need only allege "'a direct financial loss, lost dealings, or lost profits resulting from the anticompetitive acts at issue.'" *Flo & Eddie, Inc. v. Sirius XM Radio, Inc.*, 62 F. Supp. 3d 325, 349 (S.D.N.Y. 2014).

Reis's common law misappropriation claim alleges that Lennar and Rialto improperly downloaded more than 4,500 reports, which were compiled at considerable expense and labor by Reis, for which Lennar and Rialto did not pay, thereby causing Reis a direct financial loss. Compl. ¶¶ 122–30. As such, it properly alleges a misappropriation claim. Contrary to Defendants' contention, the misappropriation claim is timely, because as with conversion, the statute of limitations period becomes six years where, as here, the claim is based on fraud. *See Trustforte Corp. v. Eisen*, 10 Misc. 3d 1064(A), at *4–5.

C. Reis's Claims Against Rialto New York Are Properly Pleaded

Defendants argue that Reis's claims against Rialto New York for sharing its Reis login credentials with the Doe Unauthorized Users "all fail" because Reis "sets forth zero facts" to support its claims. Def. Br. at 24–25. Likewise, Defendants argue—incorrectly—that "[t]here is no allegation that Rialto New York breached its subscription agreement with Reis." Def. Br. at 21.

Essentially, Defendants are trying to dispute Reis's allegations on a motion to dismiss. Reis alleges that, after uncovering Lennar and Rialto's fraud involving the Lederman credentials, its Compliance Group took a closer look at the usage on Rialto New York's accounts. It was able to trace back the usage on these accounts to Rialto IP addresses, except for approximately 750 reports downloaded from two IP addresses which could not be traced back to Rialto New York. Compl. ¶ 36. Based on its experience "identify[ing] patterns of . . . unauthorized use" of its databases (*id.* ¶ 33), Reis alleges on information and belief that the usage was not by the Defendants. *Id.* ¶ 36.

Defendants' argument boils down to a claim that Reis has insufficiently detailed the basis for its allegations because it does not know the identities of the Doe Unauthorized Users. Defendants point out that IP addresses "provide[] only the location at which of one of any number of computer devices may be deployed." Def. Br. at 22 (quoting *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 84 (E.D.N.Y. 2012)). The *In re BitTorrent* cases are distinguishable. There, the plaintiff sought to sue alleged illegal downloaders of adult films. The court was naturally concerned that the copyright owners would use the stigma of being associated with pornography to extract pre-suit settlements from these defendants, without an adequate basis. *Id*. at 89 ("The most persuasive argument against permitting plaintiffs to proceed with early discovery arises from the clear indicia, both in this case and in related matters, that plaintiffs have employed abusive litigations [sic] tactics to extract settlements from John Doe defendants."). Such concerns are plainly inapposite here.

Ultimately, in any event, Defendants' arguments regarding the Rialto New York Doe Unauthorized Users are moot. As Defendants point out, Reis has sought and obtained permission from the Court to serve third-party subpoenas on the internet service providers associated with the Doe IP addresses. Def. Br. at 23–24.[11] These subpoenas have identified the Doe users as affiliated with two commercial real estate companies, Universal American Mortgage ("UAM") and JS Sullivan Development Corp. ("Sullivan"). Caplan Decl. Exs. B and D. This evidence demonstrates that Reis's allegations are not only plausible but true: the Doe Unauthorized Users are not employees of the Defendants. UAM is a sister entity of Rialto New York (but not a Reis subscriber),[12] and Sullivan is an independent real estate firm that has no conceivable legitimate reason to be using Rialto New York login credentials to access the Reis database. The facts that both the Doe Unauthorized Users are from different real estate companies than Defendants and that at least one has now been confirmed as an unauthorized user demonstrates that Reis's allegations are plausible.

IV. CONCLUSION

For the reasons described above, Defendants' motion to dismiss the Complaint should be denied.

Dated: New York, New York
December 23, 2015

By: /s/ Geoffrey Potter
Patterson Belknap Webb & Tyler LLP
Geoffrey Potter
Aron Fischer
Scott Caplan

1133 Avenue of the Americas
New York, New York 10036
(212) 336-2000
gpotter@pbwt.com
afischer@pbwt.com
scaplan@pbwt.com
Attorneys for Plaintiffs Reis, Inc. and
Reis Services, LLC

[11] Strangely, Defendants describe Reis's discovery requests as "improper." Def. Br. at 23. Reis's motion for this discovery (Dkt. 15) was unopposed, and the Court has already found Reis's requests proper and allowed them. Dkt. 16.

[12] Discovery will show whether the UAM access was authorized or not. On its face, the usage appears to be from a non-Reis subscriber.

CERTIFICATE OF SERVICE

I hereby certify that on December 23, 2015, I caused the foregoing to be electronically with the Clerk of the Court using the CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's CM/ECF system.

/s/ Scott Charles Caplan